UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

(1) an Apple iPhone 6s bearing IMEI 353253077711073 and (2) an iPhone 14 Pro bearing IMEI 35355956330430

24 MAG 2060

Case No.

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment A

located in the Southern District of New York, there is now concealed *(identify the person or describe the property to be seized)*:

Please see Attached Affidavit and its Attachment A

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☐ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 USC 371, 666, 1343, 1346, 1349; 52 USC 30121	Theft of federal funds, wire fraud, campaign contributions by foreign nationals, and conspiracy to commit these offenses

The application is based on these facts:

See Attached Affidavit and its Attachment A

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____ *)* is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

s/ [redacted] /otw
Applicant's signature

Special Agent [redacted] FBI
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone *(specify reliable electronic means)*.

Date: 05/28/2024

Judge's signature

City and state: New York, New York

Hon. Ona T. Wang, U.S.M.J.
Printed name and title

AO 93C (08/18) SDNY Rev. Warrant by Telephone or Other Reliable Electronic Means ❒ Original ❒ Duplicate Original

UNITED STATES DISTRICT COURT

for the

Southern District of New York

In the Matter of the Search of *(Briefly describe the property to be searched or identify the person by name and address)* (1) an Apple iPhone 6s bearing IMEI 353253077711073 and (2) an iPhone 14 Pro bearing IMEI 35355956330430	)	Case No. **24 MAG 2060**

WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Southern District of New York *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

The search and seizure are related to violation(s) of *(insert statutory citations)*:

18 USC §§ 371, 666, 1343, 1346, and 1349, and 52 U.S.C. § 30121

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal *(identify the person or describe the property to be seized)*:

See Attachment A

YOU ARE COMMANDED to execute this warrant on or before June 11, 2024 *(not to exceed 14 days)*

☑ in the daytime 6:00 a.m. to 10:00 p.m. ❒ at any time in the day or night because good cause has been established.

Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to the Duty Magistrate Judge .

(United States Magistrate Judge)

❒ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized *(check the appropriate box)*

❒ for _____ days *(not to exceed 30)* ❒ until, the facts justifying, the later specific date of _____ .

Date and time issued: May 28, 2024 at 6:08 pm

Judge's signature

City and state: New York, New York

Hon. Ona T. Wang, U.S.M.J.

Printed name and title

Return

Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		

Certification

I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.

Date: _____

_____
Executing officer's signature

_____
Printed name and title

Attachment A

I. The Subject Devices

The Subject Devices are particularly described as: (1) an Apple iPhone 6s bearing IMEI 353253077711073 and (2) an iPhone 14 Pro bearing IMEI 35355956330430. This warrant authorizes the extraction of data from the Subject Devices and the review of any data extracted from the Subject Devices.

II. Seizure and Review of ESI on the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the electronically stored information ("ESI") contained on the Subject Devices for evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds, bribery involving federal funds, and conspiracy to commit both), (ii) 18 U.S.C. §§ 1343, 1346 and 1349 (wire fraud, honest services fraud, and attempt and conspiracy to commit both), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the "Subject Offenses") described as follows:

1. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Devices.

2. Communications with or about [redacted] and travel in or through Turkey.

3. Financial records, including but not limited to electronic payments, credit card records, bank records, cash withdrawal records, receipts, invoices, and bills related in any way to travel to or through Turkey or using [redacted]

4. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 or 2025 New York City Mayoral campaigns of Eric Adams (the "Adams Campaigns") on the part of [redacted] Eric Adams, or anyone in communication with [redacted] or Adams.

5. Evidence relating to coordination between Turkish nationals, or the Turkish Government and the Adams Campaigns concerning political contributions to the Adams Campaigns, including, but not limited to, evidence of motive and intent for [redacted] Turkish nationals, or the Turkish Government to provide or facilitate campaign contributions to the Adams Campaign, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaigns to provide benefits, whether lawfully or unlawfully, to [redacted] Turkish nationals, or the Turkish Government in return for campaign contributions.

6. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

7. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

8. Evidence of the relationship between and among (i) [redacted] (ii) the Turkish Government, or (iii) Turkish nationals covertly contributing to the Adams Campaigns, and any person who is or was associated with or employed by the Adams Campaigns, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

9. Evidence of an intent to exchange benefits between the Turkish Government or entities and persons acting at its behest, and any person who is or was associated with or employed by [redacted] Adams, or the Adams Campaigns, including but not limited to straw donations and any actions taken by [redacted] Adams, or any person who is or was associated with or employed by the Adams Campaigns on behalf of the Turkish Government, [redacted] or entities and persons acting at the behest of the Turkish Government.

10. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Subject Devices.

11. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

12. Evidence concerning efforts to destroy evidence of the Subject Offenses or to devise or coordinate false exculpatory explanations for the conduct underlying the Subject Offenses.

B. Review of ESI

Following seizure of any electronic communications devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the device was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

24 MAG 2060

In the Matter of the Application of the United States Of America for a Search and Seizure Warrant for (1) an Apple iPhone 6s bearing IMEI 35325307771107 and (2) an iPhone 14 Pro bearing IMEI 35355956330430. USAO Reference No. 2021R00778

TO BE FILED UNDER SEAL

Agent Affidavit in Support of Application for Search and Seizure Warrant

SOUTHERN DISTRICT OF NEW YORK) ss.:

[redacted] being duly sworn, deposes and says:

I. Introduction

A. Affiant

1. I have been a Special Agent with the Federal Bureau of Investigation ("FBI") since 2019. I am currently assigned to a public corruption squad of the New York Field Office, where, among other things, I investigate crimes involving illegal campaign contributions, theft of federal funds, and bribery. Through my training and experience, I also have become familiar with some of the ways in which individuals use smart phones and electronic communications, including social media, email, and electronic messages, in furtherance of their crimes, and have participated in the execution of search warrants involving electronic evidence.

2. I make this Affidavit in support of an application pursuant to Rule 41 of the Federal Rules of Criminal Procedure for a warrant to search the electronic devices specified below (the "Subject Devices") for the items and information described in Attachment A. This affidavit is based upon my personal knowledge; my review of documents and other evidence; my conversations with other law enforcement personnel; and my training, experience and advice received concerning the use of computers in criminal activity and the forensic analysis of electronically stored information ("ESI"). Because this affidavit is being submitted for the limited

purpose of establishing probable cause, it does not include all the facts that I have learned during the course of my investigation. Where the contents of documents and the actions, statements, and conversations of others are reported herein, they are reported in substance and in part, except where otherwise indicated.

B. The Subject Devices

3. The Subject Devices are particularly described as: (1) an Apple iPhone 6s bearing IMEI[1] Apple iPhone 6s bearing IMEI 35325307771107 and (2) an iPhone 14 Pro bearing IMEI 35355956330430.

4. Based on my training, experience, and research, I know that the Subject Devices have capabilities that allow them to serve as wireless telephones, digital cameras, portable media players, GPS navigation devices, and PDAs.

5. The Subject Devices are presently located in the office of the FBI located in the Southern District of New York.

C. The Subject Offenses

6. For the reasons detailed below, I respectfully submit that there is probable cause to believe that the Subject Devices contain evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds, bribery involving federal funds, and conspiracy to commit both), (ii) 18 U.S.C. §§ 1343, 1346 and 1349 (wire fraud, honest services fraud, and attempt and conspiracy to commit both), and (iii) 18 U.S.C. § 371 and 52 U.S.C. §

[1] "IMEI," or International Mobile Equipment Identity, is a unique number used to identify certain types of cellphones. I understand that, in addition to the 14 digits listed for each IMEI here, many IMEIs may appear in the phones with which they are associated as containing one or more additional digits that may change over time. Only the first 14 unique digits are included here.

30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the "Subject Offenses").

II. Probable Cause

A. Probable Cause Regarding Subjects' Commission of the Subject Offenses

7. Since in or about August 2021, the FBI and the Office of the United States Attorney for the Southern District of New York have been investigating the receipt of so-called "straw" donations[2] by the 2021 and 2025 New York City mayoral campaigns of New York City Mayor Eric Adams, including certain straw donations that were funded by and/or made at the direction of foreign government officials and other foreign persons. As detailed more fully below and in the attached exhibits, [redacted] Turkey's Consul General in New York, was involved in facilitating at least one fundraiser at which straw donations were made. [redacted] and others associated with him, also arranged free or steeply discounted luxury travel for Adams and certain of his associates, including [redacted] [redacted] Adams's longtime romantic partner.

8. This warrant seeks permission to search two cellphones—the Subject Devices—used by [redacted] during the period in which there is probable cause to believe the Subject Offenses were committed. As detailed below, there is probable cause to believe the Subject Devices contain evidence of the Subject Offenses, including, among other things: (1) evidence that Adams, [redacted] or those acting at their behest, received a request by [redacted] to direct the New York City Department of Education to admit [redacted] son to a selective New York City public school, and (2) evidence that Adams and [redacted] among others, received free or steeply discounted luxury travel arranged by [redacted] and those associated with him.

---

[2] A straw, or "conduit," donation occurs when a donation to a political campaign is made in the name of one donor, but the funds in question in fact belong to a different person.

9. As part of this investigation, law enforcement has obtained various warrants for electronic evidence. On November 1, 2023, the Honorable James B. Clark III, United States Magistrate Judge for the District of New Jersey, issued a warrant authorizing a search of the home of [redacted] for evidence of the Subject Offenses, including any electronic devices used by [redacted] *See* Mag. No. 23-12234 (JBC) (D.N.J) (the "[redacted] Warrant"). The warrant and supporting affidavit are attached hereto as a portion of Exhibit A and incorporated by reference herein.

10. As detailed more fully in the attached affidavit for the [redacted] Warrant, this investigation has revealed, in substance and in part, the following:

a. On or about May 7, 2021, employees of [redacted] a construction company that operates in New York City, made donations to the 2021 Adams Campaign in approximately the same amount as monies paid to each of the employees by [redacted] on April 28, 2021.[3] (*See, e.g.*, [redacted] Warrant ¶¶ 9-11).

b. Many of [redacted] employees are of Turkish origin.[4] (*See, e.g.*, Ex. [redacted] Warrant ¶ 6).

c. The Adams Campaigns cultivated a relationship with [redacted] as well as the broader Turkish community, beginning at least in 2018. (*See, e.g.*, [redacted] Warrant ¶¶ 16, 19).

---

[3] Out of eleven donations from [redacted] employees made at the fundraiser, the co-owner of [redacted] who organized the fundraiser did not receive a [redacted] reimbursement check, one donor received $50 more from [redacted] than the donor donated to the 2021 Adams Campaign, and one [redacted] employee's wife donated, while the employee himself received the [redacted] reimbursement check.

[4] Certain earlier affidavits in this investigation stated that [redacted] was affiliated with a larger Turkish corporation. Law enforcement has since interviewed several [redacted] employees who have stated, in substance and in part, that although [redacted] was started by personnel formerly employed by that larger Turkish corporation, the two entities have no formal connection.

d. [redacted] was involved in fundraising for the Adams Campaigns, including arranging the fundraiser where the [redacted] straw donations were made, and communicated about fundraising with members of Adams's staff.[5] (*See, e.g.*, [redacted] Warrant ¶¶ 12(a), 12(b), 13, 16).

e. Turkish national [redacted] was involved in fundraising for the Adams Campaigns and attempted, in agreement with members of Adams's staff, to donate funds from Turkish nationals to the Adams Campaigns and communicated about fundraising with members of Adams's staff.[6] (*See, e.g.*, [redacted] Warrant ¶¶ 19-24).

f. Adams communicated with members of his staff about fundraising in the Turkish community and the potential provision of benefits to the Consul General. (*See, e.g.*, [redacted] Warrant ¶¶ 16(c), 16(j)).

g. Adams and members of his staff intervened in at least one matter within the purview of the New York City government to obtain favorable action for the Consul General; specifically, obtaining a Temporary Certificate of Occupancy ("TCO") for the official opening of a building associated with the Turkish Consulate in New York in time for a visit by Turkey's president in 2021. (*See, e.g.*, [redacted] Warrant ¶¶ 25-29).

---

[5] Certain earlier affidavits in this investigation described [redacted] and [redacted] as staff of the Adams Campaigns. Counsel for Adams has since told the Government that, at least with respect to the 2021 Adams Campaign, [redacted] was a volunteer and [redacted] was a volunteer before becoming an employee of the Campaign. As used herein, "Adams's staff" is an inclusive term referring to persons who have worked for Adams (whether as Brooklyn Borough President or Mayor) and/or the Adams Campaigns.

[6] In addition to other such donations, [redacted] assisted in coordinating straw donations from employees of [redacted] ("[redacted] a Washington, D.C.-based university partnered with a Turkish university named [redacted] Records maintained by the New York City Campaign Finance Board indicate that on September 27, 2021, five employees of [redacted] donated $2,000 each to the 2021 Adams Campaign. According to public reporting, the 2021 Adams Campaign returned the [redacted] donations approximately 17 days later, claiming that "[t]he campaign had raised more money than it could spend," but as one article notes, "campaign records show [the 2021 Adams Campaign] accepted and did not return other contributions in the weeks that followed." *See* https://www.thecity.nyc/2023/11/03/fbi-probe-eric-adams-campaign-turkey.

h. [redacted] was one of Adams's key intermediaries to the Turkish community and worked in the Special Counsel's office of the Brooklyn Borough President when Adams was Brooklyn Borough President, was involved with the Adams Campaigns, and most recently worked in the Mayor's Office for International Affairs. During the relevant time period, [redacted] had regular contact both with Turkish consular officials and with [redacted] was personally involved with the May 7, 2021 Adams fundraiser held by [redacted] at which the straw donations were made; and was personally involved in the exchange of other benefits between Adams and those associated with him and the Consul General and those associated with him. (*See, e.g.*, [redacted] Warrant ¶¶ 7, 13-18).

[redacted]

11. I know based on, among other sources, public reporting, that [redacted] is Adams's long-term romantic partner.[7] In addition, based on public reporting, I believe that at times including in or about February and March 2023, [redacted] was Senior Adviser to a Deputy Chancellor of the New York City Department of Education ("NYCDOE").[8]

12. I have reviewed the contents of an iCloud account and an Apple iPhone used by [redacted] obtained pursuant to search warrants, including text messages exchanged between [redacted] and [redacted] In February and March 2023, [redacted] ([redacted] and [redacted] ([redacted] exchanged the following text messages:

---

[7] *See, e.g.*, Sandra E. Garcia, *The 'Swagger Mayor' Attends His First Met Gala*, N.Y. Times, May 3, 2022, https://www.nytimes.com/2022/05/03/style/met-gala-party-eric-adams.html ("Mayor Eric Adams of New York was . . . accompanied by his girlfriend, [redacted] whom he introduced as his 'other half.'").

[8] *See, e.g.*, https://www.cityandstateny.com/personality/2023/06/eric-adams-friends-and-family-plush-city-jobs/387338/.

Date	From	To	
2/13/2023	[redacted]	[redacted]	Hi [redacted] Here is the contact information for the Consul General of Turkey [redacted] 4260 [redacted]
2/13/2023	[redacted]	[redacted]	Thank you so much [redacted] I will share the number with [redacted] when I see him. Please save my personal cell and I will also save your personal cell number too. Warmly, [redacted]
2/13/2023	[redacted]	[redacted]	Thank you, [redacted] Appreciate all your help
3/10/2023	[redacted]	[redacted]	Good evening [redacted] Such a pleasure to meet you today great personality and full of positive energy
3/10/2023	[redacted]	[redacted]	Here is the information for the CG's son Student Name: [redacted] Student ID: [redacted] Current School [redacted] Looking to get into M.S. 255 Salk School of Science Thank you

of NYCDOE, and that [redacted] agreed to contact [redacted] Director of Intergovernmental Affairs for NYCDOE. The conversation also indicates that [redacted] met with [redacted][9]

13. I have reviewed records from [redacted] which show, among other things, that between 2016 and 2021 [redacted] traveled with Adams to or through Turkey on approximately four occasions and on each of those occasions, [redacted] received complimentary upgrades worth several thousand dollars. Based on open-source information, I know that a sovereign wealth fund owned by the Turkish Government owns slightly less than 50% of the shares of [redacted] and is the airline's single largest shareholder.[10] I have also reviewed messages between Adams, [redacted] and others showing that [redacted] and [redacted] an officer of [redacted] operating in conjunction with [redacted] have discussed the provision of free or discounted travel benefits to Adams and those associated with him, including [redacted] (*See, e.g.*, Ex. [redacted] Warrant ¶¶ 17-18).

14. On February 20, 2024, the Honorable Sarah L. Cave, United States Magistrate Judge for the Southern District of New York, issued a warrant authorizing the seizure and search of two iCloud accounts, one of which is used by [redacted] (the "[redacted] iCloud"). The warrant and supporting affidavit (the "iCloud Warrant) are attached hereto as a portion of Exhibit A and incorporated by reference herein. Based on my review of the contents of the [redacted] iCloud obtained pursuant to that warrant, the [redacted] iCloud contains, among other things:

a. The messages discussed in ¶ 12 above, reflecting a request from [redacted] that his son be placed in the Salk School of Science.

---

[9] I understand that records maintained by the NYCDOE indicate that [redacted] son was not enrolled at Salk School of Science.

[10] [redacted]

b. Evidence of [redacted] travel, with Adams, on three trips[11] where Adams and/or [redacted] received free travel upgrades from [redacted] such as photographs of Adams and [redacted] during that travel, and messages [redacted] sent and received about that travel. These photographs and messages appear to be of the type commonly taken or sent using a cellphone.

c. Evidence that [redacted] encouraged persons she communicated with to use Signal, an electronic messaging application that can be used to conceal, encrypt, or automatically delete messages, shortly after this investigation became publicly known. Specifically, on November 2, 2023, this investigation became publicly known when FBI agents executed several search warrants, some of which drew media attention. On November 4, 2023, [redacted] exchanged messages about the execution of one of those search warrants with two individuals whom [redacted] had previously texted with. [redacted] also sent each individual a link to install Signal, which, according to the text messages, at least one of the individuals installed. Based on my experience in this investigation, I know that messages sent using Signal are often not found on a Signal user's iCloud, but can often be found on the cellphone from which the messages were sent.

B. Probable Cause Justifying Search of the Subject Devices

15. On May 17, 2024, the Honorable Leda Dunn Wettre, United States Magistrate Judge for the District of New Jersey, issued a warrant authorizing the search of a premises used by [redacted] to seize five cellphones, including the Subject Devices. That warrant (the "Seizure Warrant"), and the application for that warrant, including the affidavit in support and its exhibits

[11] The first of the four trips discussed above in paragraph 12 occurred in 2016, which is outside the date range for which the warrant for the [redacted] iCloud authorized the seizure of data.

(the application and its exhibits are collectively referred to as the "Seizure Warrant Application"), are attached as Exhibit A and incorporated by reference herein.[12]

16. On May 22, 2024, agents of the FBI executed the Seizure Warrant. I understand, based on my conversations with FBI agents who executed the Seizure Warrant, that [redacted] provided the Subject Devices to those agents, and, after consulting with an attorney by telephone, informed the agents that she no longer possessed any of the other devices named in the Seizure Warrant. [redacted] then voluntarily provided the password for both of the Subject Devices. The agents executing the Seizure Warrant then brought the Subject Devices to an FBI office in the Southern District of New York, where the Subject Devices have been maintained in materially the same condition as when seized. The agents have viewed the IMEI of each device, as authorized by the Seizure Warrant, and confirmed that the Subject Devices were two of the devices covered by the Seizure Warrant.

17. I understand, based on my review of telephone records for the telephone number used by [redacted] that [redacted] used one of the Subject Devices from approximately October 2016 to September 2018, and the other from approximately November 2022 to May 2024. As discussed above, from before 2016 to at least in or about March 2023, there is probable cause to believe that [redacted] used cellphones, including the Subject Devices, to create and/or store evidence of the Subject Offenses, including photographs and messages evincing free travel benefits provided by [redacted] to Adams and [redacted] and a request from [redacted] that New York City perform an official act at [redacted] request.

[12] The affidavit submitted in support of the Seizure Warrant relied on materially the same evidence concerning the Subject Offenses stated above in paragraphs 7 to 14, and attached and incorporated both the [redacted] Warrant and the iCloud Warrant.

18. For the reasons set forth above, there is probable cause to believe that the Subject Devices contain evidence of the Subject Offenses. In addition:

a. Cellphones can be used store documents, including emails, text messages, previous electronic chats, and financial documents like bank statements and travel expenditure. Document attachments to communications can be saved intentionally or as a result of a cellphone's operating system or web browser to an electronic device, including a cellphone. Moreover, and more generally, users of cellphones who are engaged in the commission of the Subject Offenses often store documents relevant to that activity on their devices, and also maintain notes of meetings and telephone calls on their devices. Such documents can include, but are not limited to, Microsoft Word and PDF documents, drafts, scans, bank statements received from financial institutions, and government filings.

b. Cellphones can contain photographs and videos of meetings—such as those discussed above—and documents, audio recordings of telephone calls and meetings, and screenshots of text messages.

c. Electronic files, or remnants of those files, downloaded to a cellphone can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" a file on a cellphone the data contained in the file does not actually disappear; rather, that data remains on the storage medium and within the device unless and until it is overwritten by new data. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space–that is, in space on the device that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space–for long periods of time before they are overwritten. In addition, a device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly,

files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from a cellphone depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and cellphone habits.

d. Additionally, a person can transfer data from an old cellphone, to a new device, including, for example, mail, contacts, calendars, photos and videos, books and pdfs, call logs, and text messages. For individuals who regularly change or upgrade their devices, including cellphones, it is common to transfer electronic records, such as emails, contacts, calendars, photos and videos, books and pdfs, call logs, and text messages from the old phone to a new phone. Individuals can transfer data in a few ways, including in a cellphone provider or Apple store, through a personal computer containing a backup, or through an iCloud backup. Doing so does not typically delete or remove data from the older cellphone, but rather simply duplicates it on the newer device. Accordingly, data found on one electronic device is often found on other devices used by the same person.

19. Based on the foregoing, I respectfully submit there is probable cause to believe that evidence, fruits, and instrumentalities of the Subject Offenses listed in Attachment A, which is incorporated by reference herein, will be found on the Subject Devices.

III. Procedures for Searching ESI

A. Review of ESI

20. Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government

control) will review the ESI contained on the Subject Devices for information responsive to the warrant.

21. In conducting this review, law enforcement may use various techniques to determine which files or other ESI contain evidence or fruits of the Subject Offenses. Such techniques may include, for example:

- surveying directories or folders and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);
- conducting a file-by-file review by "opening" or reading the first few "pages" of such files in order to determine their precise contents (analogous to performing a cursory examination of each document in a file cabinet to determine its relevance);
- "scanning" storage areas to discover and possibly recover recently deleted data or for deliberately hidden files; and
- performing electronic keyword searches through all electronic storage areas to determine the existence and location of search terms related to the subject matter of the investigation. (Keyword searches alone are typically inadequate to detect all information subject to seizure. For one thing, keyword searches work only for text data, yet many types of files, such as images and videos, do not store data as searchable text. Moreover, even as to text data, there may be information properly subject to seizure but that is not captured by a keyword search because the information does not contain the keywords being searched.)

22. Law enforcement personnel will make reasonable efforts to restrict their search to data falling within the categories of evidence specified in the warrant. Depending on the circumstances, however, law enforcement may need to conduct a complete review of all the ESI from the Subject Devices to locate all data responsive to the warrant.

B. Return of the Subject Devices

23. If the Government determines that the Subject Devices are no longer necessary to retrieve and preserve the data on the device, and that the Subject Devices are not subject to seizure pursuant to Federal Rule of Criminal Procedure 41(c), the Government will return the Subject Devices, upon request. Computer data that is encrypted or unreadable will not be returned unless

law enforcement personnel have determined that the data is not (i) an instrumentality of the offense, (ii) a fruit of the criminal activity, (iii) contraband, (iv) otherwise unlawfully possessed, or (v) evidence of the Subject Offenses.

IV. Conclusion and Ancillary Provisions

24. Based on the foregoing, I respectfully request the court to issue a warrant to seize the items and information specified in Attachment A to this affidavit and to the Search and Seizure Warrant.

25. In light of the confidential nature of the continuing investigation, I respectfully request that this affidavit and all papers submitted herewith be maintained under seal until the Court orders otherwise.

s/ [redacted] /otw
[redacted]
Special Agent
Federal Bureau of Investigation

Sworn to me through the transmission of this
Affidavit by reliable electronic means, pursuant to
Federal Rules of Criminal Procedure 41(d)(3) and 4.1, on

May 28, 2024

HON. ONA T. WANG
UNITED STATES MAGISTRATE JUDGE

Attachment A

I. The Subject Devices

The Subject Devices are particularly described as: (1) an Apple iPhone 6s bearing IMEI 353253077711073 and (2) an iPhone 14 Pro bearing IMEI 35355956330430. This warrant authorizes the extraction of data from the Subject Devices and the review of any data extracted from the Subject Devices.

II. Seizure and Review of ESI on the Subject Devices

A. Evidence, Fruits, and Instrumentalities of the Subject Offenses

Law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the electronically stored information ("ESI") contained on the Subject Devices for evidence, fruits, and instrumentalities of violations of (i) 18 U.S.C. §§ 371 and 666 (theft of federal funds, bribery involving federal funds, and conspiracy to commit both), (ii) 18 U.S.C. §§ 1343, 1346 and 1349 (wire fraud, honest services fraud, and attempt and conspiracy to commit both), and (iii) 18 U.S.C. § 371 and 52 U.S.C. § 30121 (campaign contributions by foreign nationals and conspiracy to commit the same) (collectively, the "Subject Offenses") described as follows:

1. Evidence concerning the identity or location of the owner(s) or user(s) of the Subject Devices.

2. Communications with or about [redacted] and travel in or through Turkey.

3. Financial records, including but not limited to electronic payments, credit card records, bank records, cash withdrawal records, receipts, invoices, and bills related in any way to travel to or through Turkey or using [redacted]

4. Evidence of knowledge or understanding of, or intent to violate, laws and regulations governing the conduct of the 2021 or 2025 New York City Mayoral campaigns of Eric Adams (the "Adams Campaigns") on the part of [redacted] Eric Adams, or anyone in communication with [redacted] or Adams.

5. Evidence relating to coordination between Turkish nationals, or the Turkish Government and the Adams Campaigns concerning political contributions to the Adams Campaigns, including, but not limited to, evidence of motive and intent for [redacted] Turkish nationals, or the Turkish Government to provide or facilitate campaign contributions to the Adams Campaign, and evidence of motive and intent by any person who is or was associated with or employed by the Adams Campaigns to provide benefits, whether lawfully or unlawfully, to [redacted] Turkish nationals, or the Turkish Government in return for campaign contributions.

6. Evidence of individuals or entities who donated to the Adams Campaign before or after receiving transfers of funds similar to the amount of the donation.

7. Evidence regarding the identity of any persons or entities involved, wittingly or unwittingly, in straw donations to the Adams Campaign.

8. Evidence of the relationship between and among (i) [redacted] (ii) the Turkish Government, or (iii) Turkish nationals covertly contributing to the Adams Campaigns, and any person who is or was associated with or employed by the Adams Campaigns, including all communications with or about, contact information for, and meetings and appointments with co-conspirators.

9. Evidence of an intent to exchange benefits between the Turkish Government or entities and persons acting at its behest, and any person who is or was associated with or employed by [redacted] Adams, or the Adams Campaigns, including but not limited to straw donations and any actions taken by [redacted] Adams, or any person who is or was associated with or employed by the Adams Campaigns on behalf of the Turkish Government, [redacted] or entities and persons acting at the behest of the Turkish Government.

10. Passwords or other information needed to access the user's online accounts, including encrypted data stored in the Subject Devices.

11. Evidence of the geographic location of users, computers, or devices involved in the commission of the Subject Offenses at times relevant to the Subject Offenses.

12. Evidence concerning efforts to destroy evidence of the Subject Offenses or to devise or coordinate false exculpatory explanations for the conduct underlying the Subject Offenses.

B. Review of ESI

Following seizure of any electronic communications devices and/or the creation of forensic image copies, law enforcement personnel (who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, agency personnel assisting the government in this investigation, and outside technical experts under government control) are authorized to review the ESI contained therein for information responsive to the warrant.

In conducting this review, law enforcement personnel may use various techniques to locate information responsive to the warrant, including, for example:

- surveying various file "directories" and the individual files they contain (analogous to looking at the outside of a file cabinet for the markings it contains and opening a drawer believed to contain pertinent files);

- opening or cursorily reading the first few "pages" of such files in order to determine their precise contents;

- scanning storage areas to discover and possibly recover recently deleted files or deliberately hidden files;

- performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are intimately related to the subject matter of the investigation; and

- reviewing metadata, system information, configuration files, registry data, and any other information reflecting how, when, and by whom the device was used.

Law enforcement personnel will make reasonable efforts to search only for files, documents, or other electronically stored information within the categories identified in Section II.A of this Attachment. However, law enforcement personnel are authorized to conduct a complete review of all the ESI from seized devices or storage media if necessary to evaluate its contents and to locate all data responsive to the warrant.

Exhibit A

[24-mj-13089]